

Please type a plus sign (+) inside this box →

Based on PTO/SB/05 (4/98)

Approved for use through 09/30/2000. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No. 11953.0002

First Inventor or Application Identifier David A. PENSAK

Title INFORMATION SECURITY ARCHITECTURE FOR ENCRYPTING DOCUMENTS FOR REMOTE ACCESS WHILE MAINTAINING

Express Mail Label No. 

APPLICATION ELEMENTS

See MPEP Chapter 600 concerning utility patent application contents.

1. Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original, and a duplicate for fee processing)

2. Specification [Total Pages 21]
[preferred arrangement set forth below]
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R&D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. Drawing(s) (35 U.S.C. 113) [Total Sheets 2]
[

4. Oath or Declaration [Total Pages]
[

a. Newly executed (original or copy)
b. Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)

i. **DELETION OF INVENTOR(S)**
Signed statement attached deleting
inventor(s) named in the prior application,
see 37 CFR §§1.63(d)(2) and 1.33(b).

***NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28)**

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

5. Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. Computer Readable Copy
b. Paper Copy (identical to computer copy)
c. Statement verifying identical of above copies

ACCOMPANYING APPLICATION PARTS

7. Assignment Papers (cover sheet & documents(s))
8. 37 CFR §3.73(b) Statement Power of Attorney
[when there is an assignee]
9. English Translation Document (if applicable)
10. Information Disclosure Statement (IDS)/PTO-1449 Copies of IDS Citations
11. Preliminary Amendment
12. Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
*Small Entity Statement filed in prior application,
Statements(s) Status still proper and desired
(PTO/SB/09-12)
13. Certified Copy of Priority Document(s)
(if foreign priority is claimed)
14. Other _____
15. Other _____

16. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below and in a preliminary amendment:

Continuation Divisional Continuation-in-part (CIP)

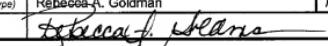
of prior application No. /

Prior application information Examiner _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon which a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

Name	Stuart T.F. Huang STEPTOE & JOHNSON LLP				
Address	1330 Connecticut Avenue, N.W.				
City	Washington	State	DC	Zip Code	20035
Country	US	Telephone	202-429-3000	Fax	202-429-3902

Name (Print/Type)	Rebecca A. Goldman	Registration No. (Attorney/Agent)	41,786
Signature		Date	May 28, 1999

APPLICATION UNDER UNITED STATES PATENT LAWS

Invention: INFORMATION SECURITY ARCHITECTURE FOR ENCRYPTING DOCUMENTS FOR REMOTE ACCESS WHILE MAINTAINING ACCESS CONTROL

Inventor(s): David A. PENSAK

Attorneys:

Steptoe & Johnson LLP
1330 Connecticut Avenue, NW
Washington, DC 20036-1795
Tel. (202) 429-3000
Fax. (202) 429-3902

This is a:

- Provisional Application
- Regular Utility Application
- Continuing Prosecution Application
- PCT National Phase Application
- Design Application
- Reissue Application
- Plant Application

METHOD OF ENCRYPTING INFORMATION FOR REMOTE ACCESS WHILE
MAINTAINING ACCESS CONTROL

BACKGROUND

5 This invention relates to an electronic security system for electronic objects such as documents, video and audio clips and other objects that can be transmitted via a network.

10 Electronic security systems have been proposed for managing access to electronic information and electronic documents so that only authorized users may open protected information and documents. Several software tools have been developed to work with particular document readers such as Adobe Acrobat Exchange and Adobe Acrobat Reader.

15 A need still exists for improved systems for providing access to encrypted information by authorized users and which prevent unauthorized users from gaining access to the encrypted information. The present invention allows the authoring user or other controlling party to maintain access 20 control over the electronic information.

SUMMARY

25 The preferred embodiment(s) of the invention are summarized here to highlight and introduce some aspects of the present invention. Simplifications and omissions may be made in this summary. Such simplifications and omissions are not intended to limit the scope of the invention.

30 The object of the present invention is to provide a system and method for encrypting electronic information so that access to the information can be controlled by the author or other controlling party.

A further object of the present invention is to provide an electronic encryption/decryption system and method in which a central server maintains control over the electronic encryption and decryption keys.

5 A further object of the present invention is to provide an electronic encryption/decryption system and method in which electronic encryption and decryption keys are not retained by an encrypting or decrypting party.

10 A further object of the present invention is to provide a system and method for encrypting electronic information so that access to the information can be dynamically changed from a single location without the necessity of collecting or redistributing the encrypted information.

15 A further object of the present invention is to provide an electronic encryption/decryption system and method in which access to electronic information can be permanently revoked by destroying the association of a decryption key to the electronic information.

20 These and other objects will become apparent from the figures and written description contained herein.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiment(s) of the invention will be 25 discussed below with reference to attached drawings in which:

FIG. 1 is a block diagram illustrating a system configuration of an authoring tool, a viewing tool, and a remote server of the electronic encryption system.

30 FIG. 2 is a block diagram illustrating a detailed system configuration and functions associated with each component of the electronic encryption system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

Referring now to the Figures wherein like reference numerals indicate like elements, in FIG. 1, the system of the preferred embodiment can be broken down conceptually

5 into three functional components: an authoring tool 102, a viewing tool 104, and a remote server 106. For convenience, the embodiments described herein are described with respect to a document in Adobe Acrobat Exchange, but other embodiments using other base software packages are possible.

10 Other types of electronic information, as determined by the base software package chosen, can be encrypted using the present invention.

The authoring tool 102 allows an authoring user 108 to convert a text document 110 to unreadable form 112 using a

15 strong encryption algorithm and an encryption key, or set of encryption keys, provided by the remote server 106. The authoring tool 102 also registers the electronic document or information with the remote server 106 and associates a set of access policies with the encryption key so that only

20 selected viewing users 116 under selected circumstances may view the document in clear text. The document or information may also be broken down into segments using the authoring tool 102, so that certain segments within a document may have different access policies. For example, a

25 set of users may be allowed to view pages 1-5 of a 10 page document in clear text, while a subset of those users may be allowed to view all 10 pages of the document. The authoring tool 102 also allows the authoring user 108 to block certain functions normally accessible by the viewing user 116. For

30 example, the authoring user 108 may deny a viewing user 116 privileges such as printing and copying of the clear text.

The viewing tool 104 allows a viewing user 116 to decrypt the document 112 an authoring user 108 has encrypted, provided the authoring user 108 has associated an access policy with the decryption key which grants access to 5 the clear text to the viewing user 116. The viewing tool 104 retrieves the decryption key 118 associated with the document segment 112 from the remote server 106, decrypts the document into clear text, renders the document segment, and destroys the decryption key and the clear text version 10 of the document segment. The viewing tool 104 prevents the saving of the decryption key or the clear text version of the document. The viewing tool 104 also blocks the viewing user's machine from performing certain functions, such as printing or copying, as directed by the authoring user 108 15 during registration of the document 110.

The secure remote server 106 performs several functions. The remote server 106 generates encryption keys 114 for each document segment, maintains decryption keys 118 for registered encrypted documents 112, authenticates 20 requests for viewing a document segment, grants access to registered documents 112 by providing decryption keys 118 and associated access policies to authorized viewing users 116, and maintains an encrypted secure central database which provides association between registered authoring 25 users, registered documents, associated decryption keys, associated policies for each document, options for each user and document, and associated registered viewing users. The remote server 106 does not store or receive the actual document, either encrypted or unencrypted.

30 The authoring tool 102 and the viewing tool 104 each use essentially the same suite of software tools. As shown in FIG. 2, the software tools reside on the authoring and

668251-668251-20060

viewing users' computers 222, 224. Registration with the central remote server 206 determines which functions within the suite of software tools are available to a particular user. The software tools include a Configuration Utility 226, an Administrator Utility 228, and an Application Interface 230. In the embodiment using Adobe Acrobat Exchange, the Application Interface is a "Plug-In," which uses SDK and Plug-In Standard Interface. The three software tools run in conjunction with base viewing or playback software 232, such as Adobe Acrobat Exchange, a web browser, a word processor, an audio or video playing application, a custom data processing, or a specialized low-level device driver, such as a hard disk driver, video driver, or audio driver. The base software package 232 will depend on the 10 type of data stream to be encrypted/decrypted.

THE SECURE REMOTE SERVER

The secure remote server 206 is a server which is remote from an authoring or viewing user 208, 216. The 20 server 206 maintains a database 236 of encryption keys and associated decryption keys for distribution to registered or authorized users. The remote server 206 also maintains a database which associates registered document segments, which are identified by unique segment IDs, with authoring 25 users, user access profiles, document access policies and options, and associated encryption/decryption keys. The remote server 206 does not actually store registered documents or segments, but instead relates identifying information about a document to the associated information.

The remote server 206 also tracks and maintains records 30 of requests to view documents and to obtain document decryption keys 238. The records may be used to monitor the

system for suspicious activity. For example, a single user requesting the decryption key for a document several times during a specific time period might be an indication of suspicious activity. The server can then provide an alert 5 message to a pager, e-mail or fax, thus allowing timely investigation of the activity. The request information may also be used for the purposes of non-repudiation or as a basis for billing in situations where access to the system or access to protected information is being sold.

10 All communication between the remote server 206 and a user's computer 222, 224 is encrypted using Secure Socket Layer (SSL) protocols. Once an SSL tunnel has been negotiated between a user's machine 222, 224 and the secure server 206, a session key is negotiated. Thus, 15 communications to and from the secure server 206 and a user's computer 222, 224 are doubly encrypted.

Registration with the remote server 206 of a user or automated system wishing to use the system is done separately from any communication for registering a document 20 or viewing a document. A user wishing to register documents for viewing by other users, or viewing registered document registered by other users, must contact the server independently, possibly through a separate human Coordinator 240 or separate network link which can collect payment for 25 the authoring, viewing, and other services, can verify the identity of the user and provide the server with user identification information and user authorization profiles.

The server may be a single server, a set of synchronized servers, or dual servers with a shared 30 database.

THE CONFIGURATION UTILITY

The Configuration Utility 226 defines a local user (authoring or viewing) on the user's computer 222, 224. The Configuration Utility 226 establishes the communication 5 parameters for a local user and the remote server 206. For example, the Configuration Utility 226 will query the user to define a local user profile, to include name, password and other identifying information. This local user profile must match the information provided by a user to the 10 Coordinator 240 at the remote server 206.

The Configuration Utility 226 is also responsible for maintaining information regarding the authentication and secure communication method used by the local user, for example, certificate, secret passphrase, smart card, etc. 15 The Configuration Utility 226 maintains information about the local user's secure communication method, for example, the certificate and certification authority for a certificate based secure communication system.

20 THE ADMINISTRATOR UTILITY

The Administrator Utility 226 is a network client application used by the human Coordinator 240 and other users to control access to documents selected for encryption by defining policies associated with a document. The 25 Administrator Utility 228 is a software program residing on the user's computer 222, 224. The Coordinator 240 or authoring user 208 uses the Administrator Utility 228 to define policies related to a particular user. For example, the Coordinator 240 can use the Administrator Utility 228 to 30 control the functions available to a particular authoring user 208, which might depend on the fees paid by the authoring user 208, or the Coordinator 240 can control the

amount of access an authoring user 208 can allow to viewing users 216. Other policies that an individual can define using the Administrator Utility 228 are site policies, group policies, and default policies.

5 The Administrator Utility 228 allows the Coordinator 240 or authoring or viewing user 208, 216 to determine what documents have been registered by a particular user by accessing the registered user database 236. The Administrator Utility 228 also allows an authoring user to 10 permanently disable the viewing of documents by deleting the associated decryption key from the server. The Administrator Utility 228 also allows an authoring user 208 to initially define the policies related to his documents and to change the policies after the documents have 15 initially been registered.

 The Administrator Utility 228 allows a normal authoring user 208 to create, edit, and delete time windows, network specifications and policy templates; view the list of registered documents; and view and edit the policies of 20 documents that are registered. The Administrator Utility 228 allows the Coordinator 240 to create, edit, and delete users and user policies; create, edit, and delete groups of users and group policies; create, edit, and delete document groups and document group policies; define and modify the 25 Site and Default policies; create, edit, and delete document override policies; and view the activity log and set up notification policies

THE APPLICATION INTERFACE

30 The Application Interface 230 of the preferred embodiment is a standard "Plug-In" to Adobe Acrobat Exchange using SDK and Plug-In Standard Interface. The Plug-In 230

provides a user screen interface to allow the user to access the particular functions associated with registering and viewing documents and communicating with the server. The Plug-In Screen may be integral to the Adobe User Interface 5 Window or may be a separate window. In the preferred embodiment, the Plug-In 230 modifies the Adobe User Interface Window by adding functional "buttons" such as register, create policies, tag, encrypt, view and decrypt.

10 The Plug-In 230 allows encryption and decryption of PDF files using encryption keys from the remote server 206. The Plug-In 230 connects to the server 206, authenticates the user to the server, registers documents with the server, selects policies at the server as they have been defined by the authoring user 208 using the Administrator Utility 228.

15 In addition, the Plug-In 230 blocks certain functions at the viewing user's computer 224 that are otherwise available in Adobe Acrobat Exchange. For example, if the authoring user 208 has limited access to a document so that a viewing user 216 is prohibited from printing a viewed 20 document, the Plug-In 230 temporarily disables the print function of Adobe Acrobat Exchange. Among the functions that the Plug-In 230 can disable are print, copy, cut, paste, save, and other functions. Other functions may be disabled or limited as appropriate for the type of file 25 viewed and the access level. The Application Interface 230 is designed in such a way that it does not disclose either the decryption key or the clear text or unencrypted representation of the protected information content in electronic form.

THE GRAPHICAL USER INTERFACE

The Graphical User Interface ("GUI") supports standard user interface objects such as push buttons, text input fields, lists, menus, and message boxes. The GUI is controlled by the mouse and keypad. The GUI has multiple windows that allow real time setup of server configuration such as who may register a document, who may view a document, when a document may be viewed and on which host the document key and viewing information resides.

10

INITIAL USER SETUP

A user who wishes to register or to access information must first register and be recognized by the server 206, as represented by reference numeral 1042, 1044 in FIG. 2. The user 208, 216 contacts the server 206 independently, possibly through a separate human Coordinator 240 or separate network link which can collect payment for the authoring, viewing and other services; verify the identity of the user; and provide the server with user identification information and user authorization profiles. Once the user 208, 216 is registered with the server 206, the suite of software tools is provided to the user.

The user must have installed the base software 230, such as Adobe Acrobat Exchange, on his computer. The user then installs the Application Interface 230 provided by the Coordinator 240, as well as the Administrator and Configuration Utilities 228, 226. In one embodiment, upon running the Application Interface 230, the Application Interface 230 will install the Administrator and Configuration Utilities 228, 226 on the user's machine. There is no network activity involved in the installation of

the Application Interface 230, Administrator, or Configuration Utilities 228, 226.

CREATING POLICIES USING THE ADMINISTRATOR

5 Once a user 208, 216 is registered and the Configuration Utility 226 has set up identification and encryption information for the user 208, 216, the user authorized to do so can use the Administrator Utility 228 to create policies associated with a specific document. An 10 authoring user 208 wishing to register a document creates policies to define who, when and how a document may be viewed or otherwise accessed.

The authoring user 208 runs the Administrator Utility 228 which has been installed on his machine 222 and 15 instructs the Administrator Utility 228 to create policies for a document. The Administrator Utility 228 will request the information provided during set up to the Configuration Utility 226 such as username, passphrase, and method of authentication to verify the user's identity. The 20 Administrator Utility 228 will also ask on which server the authoring user 208 wishes to register his document. The Administrator Utility 228 will then establish a connection to the remote server through the Application Interface 230.

25 The remote server 206 and the authoring or viewing user's computer 222, 224 communicating with the server 206 will negotiate a standard Secure Socket Layer (SSL) encryption tunnel, as represented in FIG.2 by reference numerals 1046, 1056.

Once the SSL tunnel is established, the user's computer 30 222, 224 and the server 206 negotiate a secondary session key, as represented in FIG.2 by reference numerals 1048, 1058. All subsequent communications is additionally

encrypted using 128-bit RC4 and this secondary session key. All communication between the users' computers 222, 224 and the server 206 is thus doubly encrypted.

Once the doubly encrypted communication link is
5 established between the authoring user's computer 222 and the server 206, the authoring user's computer 222 provides login and authentication information to the server 206, 1050. The server 206 authenticates the authoring user's 208 identity and verifies that the authoring user 208 has
10 authority to use the system by checking a database of registered users 236 maintained on the server. The information provided by the authoring user 208 to the Configuration Utility 226 is compared to the information provided by the user to the Coordinator 240 during the
15 independent user registration process 1042, 1044. The database 234 contains all of the access controls related to a particular user, so that if a user is only authorized to view documents, he will not be allowed to use the system to register or encrypt documents.

20 After the server 206 authenticates the authoring user 208 and verifies that the authoring user 208 is authorized to register documents, the Administrator Utility 228 allows the authoring user 208 to create policies applicable to a particular viewing user 216, a group of viewing users, or a
25 default policy for all other users. The policies are then communicated to the server 206, 1051. Policies define who may view a document, when, and under what conditions. Policies are created by combining a set of constraints including allowable or denied users and groups, time ranges,
30 and Internet Protocol (IP) addresses. Access to a document by a viewing user 216 is determined by combining the user policy, document policy, as well as possibly the group

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

policy and document group policy. If the Coordinator 240 has created a document override policy for a document, then the override takes precedence over the regular document policy defined by the authoring user. Policies include

5 limiting who may view a document or portion of a document and the time frame during which a user may view the document.

The Administrator Utility 228 also allows the authoring user 208 to create options. Options specify what functions

10 of the base software 232 are temporarily disabled so that the viewing user 216 is prohibited from accessing them while viewing the document. An option can also enforce a watermark on printing. For example, the authoring user 208 can prohibit a particular viewing user 216 from printing, 15 saving, or copying a particular document or portion of a document. These Options are defined by the authoring user 208 using the Administrator Utility 228, but the options are enforced by the Application Interface 230.

20 ENCRYPTING DOCUMENTS AND DATA STREAMS

An authoring user 208 wishing to encrypt a document will open the document on his computer 222. The Application Interface 230 must also be loaded before the document or information can be encrypted. In the preferred embodiment,

25 the Plug-In 230 adds menu items to the menu bar in Adobe Acrobat Exchange such as "tag" and "encrypt." "Tag" allows the authoring user 208 to select segments of the document to be encrypted. The authoring user 208 can assign different policies to different tagged segments of a single document, 30 i.e., policies are associated with segments. A segment may consist of any subset of the entire document or the entire document. Once the document has been segmented or "tagged,"

the authoring user selects "encrypt" from the menu bar. If the authoring user 208 has not already logged into the remote server 206, the Plug-In 230 will force a log in to the remote server 206 through the Administrator Utility 228.

5 A log-in screen is provided and the authoring user 208 must log-in to the server 206. The server 206 authenticates the authoring user 208 and verifies that the authoring user 208 is authorized to register documents.

Once the authoring user has been authenticated, the
10 authoring user is asked to associate the overall document with a policy, and this information is communicated to the remote server 1052. This policy becomes the default policy for any portions of the document which are not tagged and associated with a specific policy. The Plug-In 230 assigns
15 a unique segment ID for each tagged segment after the authoring user has tagged all segments and has instructed the Plug-In 230 to go ahead with the encryption. The Plug-In 230 transmits the segment IDs to the server 206. The server 206 generates a random encryption key for each
20 segment ID and communicates the encryption key to the authoring user's computer 222, 1054. The server 206 stores the segment ID, the key associated with the particular segment ID, and the policy associated with a particular segment ID in the central database 234, and then transmits
25 the key to the Plug-In 230 at the authoring user's computer 222. The Plug-In 230 at the authoring user's computer 222 encrypts the segment, immediately destroys or removes the key from the authoring user's machine 222, and then deletes the clear text for the segment from the Plug-In 230. Thus,
30 key lifetime is very short on the authoring user's machine. The encryption key is never stored on the authoring user's machine where it is accessible, such as the hard disk. The

1000
999
998
997
996
995
994
993
992
991
990
989
988
987
986
985
984
983
982
981
980
979
978
977
976
975
974
973
972
971
970
969
968
967
966
965
964
963
962
961
960
959
958
957
956
955
954
953
952
951
950
949
948
947
946
945
944
943
942
941
940
939
938
937
936
935
934
933
932
931
930
929
928
927
926
925
924
923
922
921
920
919
918
917
916
915
914
913
912
911
910
909
908
907
906
905
904
903
902
901
900
899
898
897
896
895
894
893
892
891
890
889
888
887
886
885
884
883
882
881
880
879
878
877
876
875
874
873
872
871
870
869
868
867
866
865
864
863
862
861
860
859
858
857
856
855
854
853
852
851
850
849
848
847
846
845
844
843
842
841
840
839
838
837
836
835
834
833
832
831
830
829
828
827
826
825
824
823
822
821
820
819
818
817
816
815
814
813
812
811
810
809
808
807
806
805
804
803
802
801
800
799
798
797
796
795
794
793
792
791
790
789
788
787
786
785
784
783
782
781
780
779
778
777
776
775
774
773
772
771
770
769
768
767
766
765
764
763
762
761
760
759
758
757
756
755
754
753
752
751
750
749
748
747
746
745
744
743
742
741
740
739
738
737
736
735
734
733
732
731
730
729
728
727
726
725
724
723
722
721
720
719
718
717
716
715
714
713
712
711
710
709
708
707
706
705
704
703
702
701
700
699
698
697
696
695
694
693
692
691
690
689
688
687
686
685
684
683
682
681
680
679
678
677
676
675
674
673
672
671
670
669
668
667
666
665
664
663
662
661
660
659
658
657
656
655
654
653
652
651
650
649
648
647
646
645
644
643
642
641
640
639
638
637
636
635
634
633
632
631
630
629
628
627
626
625
624
623
622
621
620
619
618
617
616
615
614
613
612
611
610
609
608
607
606
605
604
603
602
601
600
599
598
597
596
595
594
593
592
591
590
589
588
587
586
585
584
583
582
581
580
579
578
577
576
575
574
573
572
571
570
569
568
567
566
565
564
563
562
561
560
559
558
557
556
555
554
553
552
551
550
549
548
547
546
545
544
543
542
541
540
539
538
537
536
535
534
533
532
531
530
529
528
527
526
525
524
523
522
521
520
519
518
517
516
515
514
513
512
511
510
509
508
507
506
505
504
503
502
501
500
499
498
497
496
495
494
493
492
491
490
489
488
487
486
485
484
483
482
481
480
479
478
477
476
475
474
473
472
471
470
469
468
467
466
465
464
463
462
461
460
459
458
457
456
455
454
453
452
451
450
449
448
447
446
445
444
443
442
441
440
439
438
437
436
435
434
433
432
431
430
429
428
427
426
425
424
423
422
421
420
419
418
417
416
415
414
413
412
411
410
409
408
407
406
405
404
403
402
401
400
399
398
397
396
395
394
393
392
391
390
389
388
387
386
385
384
383
382
381
380
379
378
377
376
375
374
373
372
371
370
369
368
367
366
365
364
363
362
361
360
359
358
357
356
355
354
353
352
351
350
349
348
347
346
345
344
343
342
341
340
339
338
337
336
335
334
333
332
331
330
329
328
327
326
325
324
323
322
321
320
319
318
317
316
315
314
313
312
311
310
309
308
307
306
305
304
303
302
301
300
299
298
297
296
295
294
293
292
291
290
289
288
287
286
285
284
283
282
281
280
279
278
277
276
275
274
273
272
271
270
269
268
267
266
265
264
263
262
261
260
259
258
257
256
255
254
253
252
251
250
249
248
247
246
245
244
243
242
241
240
239
238
237
236
235
234
233
232
231
230
229
228
227
226
225
224
223
222
221
220
219
218
217
216
215
214
213
212
211
210
209
208
207
206
205
204
203
202
201
200
199
198
197
196
195
194
193
192
191
190
189
188
187
186
185
184
183
182
181
180
179
178
177
176
175
174
173
172
171
170
169
168
167
166
165
164
163
162
161
160
159
158
157
156
155
154
153
152
151
150
149
148
147
146
145
144
143
142
141
140
139
138
137
136
135
134
133
132
131
130
129
128
127
126
125
124
123
122
121
120
119
118
117
116
115
114
113
112
111
110
109
108
107
106
105
104
103
102
101
100
99
98
97
96
95
94
93
92
91
90
89
88
87
86
85
84
83
82
81
80
79
78
77
76
75
74
73
72
71
70
69
68
67
66
65
64
63
62
61
60
59
58
57
56
55
54
53
52
51
50
49
48
47
46
45
44
43
42
41
40
39
38
37
36
35
34
33
32
31
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1

key can even be obfuscated while in the memory of the authoring user's machine. The duration of the key's existence depends on the speed of the computer which actually performs the encryption, since the key is destroyed
5 immediately after the encryption. In the preferred embodiment, 128-bit RC4 is used for document and segment encryption.

Once all segments have been encrypted, the Plug-In 230 produces a hash of the entire document and sends the hash to
10 the server as document identification, 1055. The server 206 stores the hash with the keys associated with the document. Thus, the document is never transmitted to the server 206, only the segment IDs and hash.

15 A pop-up window asks the authoring user 208 where he wishes to store the encrypted document. By default, the encrypted document overwrites the clear text document on the authoring user's machine 222.

VIEWING, REPLAYING, AND DECRYPTING

20 A user wishing to view a document must have installed the Configuration Utility 226, Administrator Utility 228, and the Application Interface 230 on his computer 224. The viewing user 216 must be independently registered with the Coordinator 240 as a user. The viewing user 216 must also
25 have installed the base software application 232 for viewing the document, such as Adobe Acrobat Exchange. The viewing user 216 must enter the Configuration Utility 226 and provide user set up information.

If the viewing user 216 has not opened the
30 Configuration Utility 226, the Administrator Utility 228 and the Application Interface 230, these programs will automatically be opened once the information to be accessed

668517 668517 668517 668517 668517

has been selected, and the system has recognized that the information is encrypted.

Once the Configuration Utility 226 has opened, it will request the user to provide information defining both the viewing user 216 and the viewing user's computer 224. If the viewing user 216 is a new user, the viewing user 216 will select a button on the Configuration Utility's interface window indicating that a new user profile needs to be provided. The Configuration Utility 226 will provide a query screen to the user and the user will input identification information, such as a user name. The identification information will be checked against the information provided to the server 206 or Coordinator 240 during the independent user registration process.

The Application Interface 230 will check to see if the user is logged onto the remote server 206. If the viewing user 216 has not logged onto the remote server, the Application Interface 230 provides a pop-up window so that the user can log in to the server. An SSL tunnel and session key are negotiated, 1056, 1058. The viewing user's computer 224 provides login and authentication information to the server 206, 1060. Once logged into the server 206, the Application Interface 230 requests access to the document or information 1062 by asking the server 206 for the decryption key for the first segment of the document or information to be accessed. The server 206 uses the segment ID to check the database to find the policies associated with the segment and thus to determine whether the viewing user 216 is authorized to access this segment or the document as a whole.

If the viewing user 216 is not authorized to access the segment, the viewing user 216 is so informed. If the user

SEARCHED
SERIALIZED
INDEXED
FILED
606

216 is authorized to access the segment, the server 206
sends the decryption key and options for that segment to the
Application Interface 230 at the viewing user's computer 224
and the Application Interface 230 decrypts the segment using
5 the decryption key. After decrypting the segment, the
Application Interface 230 immediately discards/destroys the
key, renders the decrypted segment to the screen, and then
destroys the decrypted version of the segment. When the
viewing user moves to a different segment, the process is
10 repeated.

The Application Interface 230 enforces the options
which were assigned by the authoring user 230 to the segment
viewed by the viewing user 216. For example, if the
authoring user 208 assigned that the viewing user 216 cannot
15 print the clear text document or segment, then the Plug-In
230 disables the print function of Adobe Acrobat Exchange
while the clear text document or segment is available to the
viewing user 216. Other functions which can be controlled
or disabled by the Plug-In 230 are save, copy, paste, and
20 print with watermark. For other base software packages such
as audio 230, the functions controlled by the Application
Interface 230 could be play, copy, and save unencrypted.
Thus, using the options, the viewing user 216 has no ability
to permanently acquire the clear text document or data.

25

THE DATABASE

The secure central database 234 resides on the remote
server 206. It may be a distributed or shared database
residing on multiple remote servers 206. In the preferred
30 embodiment the database 234 is maintained in Berkley DB
software. All records maintained in the central database
234 are encrypted and the database is password protected.

The Coordinator 240 controls the database 234 and has access to the database 234 using the password.

All keys for encryption and decryption are maintained in the database 234. The database 234 provides a structure 5 for associating segment IDs with an associated decryption key, policies for accessing that segment, and options for accessing that segment. The authoring user 208 may change a policy associated with a segment ID through the Administrator Utility 228 on his computer. The change in 10 policy is communicated to the remote server 206 and the database 234 is updated accordingly. The update policy function allows an authoring user 208 to revoke access to a segment or document by a user or group of users.

The authoring user 208 can destroy the decryption key 15 or the association of a decryption key to a segment or document on the database 234 using the Administrator Utility 228. By destroying the decryption key or the association of the decryption key with a Segment or Document, the authoring user 208 destroys the ability to decrypt the information, 20 effectively shredding all copies of the information.

Regular backups of the database 234 are made without shutting down the whole database 234.

One or more preferred embodiments have been described to illustrate the invention(s). Additions, modifications, 25 and/or omissions may be made to the preferred embodiment(s) without departing from the scope or spirit of the invention(s). It is the intent that the following claims encompass all such additions, modifications, and/or variations to the fullest extent permitted by law.

668290 668291 668292 668293 668294 668295 668296

WHAT IS CLAIMED IS:

1. A method of controlling distribution of electronic information comprising the steps of:

5 retrieving, at a user location, a segment of encrypted electronic information;
receiving, from a key server, (a) a copy of a decryption key for the segment, and (b) at least one user limitation assigned to the segment and associated with the decryption key;
10 accessing the segment using the copy of the decryption key at the user location for the segment and a control process, the control process responsive to a user limitation to control distribution of the electronic information; and
15 destroying the copy of the decryption key at the user location after accessing the segment.

2. The method of controlling distribution of electronic information of claim 1, wherein access to the decryption key is controlled by the key server subject to a unique segment identification associated with the segment and the user limitation associated with the segment.

25 3. A method of accessing first and second encrypted segments of an electronic document comprising the steps of: retrieving, at the user location, a first encrypted segment of the electronic document; receiving, from a key server, (a) a copy of a first
30 decryption key for the first segment and (b) at least one user limitation assigned to the first

segment and associated with the first decryption key;

accessing the first segment using the copy of the first decryption key for the first segment; and

5 at the user location, destroying the copy of the first decryption key for the first segment as a precondition to receiving a decryption key for accessing a second segment of the electronic document.

0924439-052894

ABSTRACT

The invention provides for encrypting electronic information such as a document so that only users with 5 permission may access the document in decrypted form. The process of encrypting the information includes selecting a set of policies as to who may access the information and under what conditions. A remote server stores a unique identifier for the information and associates an 10 encryption/decryption key pair and access policies with the information. Software components residing on the author's computer retrieve the encryption key from the remote server, encrypt the information, and store the encrypted information at a location chosen by the author. A user wishing to access 15 the information acquires the encrypted information electronically. Software components residing on the viewing user's computer retrieve the associated decryption key and policies, decrypt the information to the extent authorized by the policies, and immediately delete the decryption key 20 from the viewing user's computer upon decrypting the information and rendering the clear text to the viewing user's computer screen. The software components are also capable of prohibiting functional operations by the viewing user's computer while the clear text is being viewed.

60623569
60623570
60623571
60623572
60623573
60623574
60623575
60623576
60623577
60623578
60623579
60623580
60623581
60623582
60623583
60623584
60623585
60623586
60623587
60623588
60623589
60623590
60623591
60623592
60623593
60623594
60623595
60623596
60623597
60623598
60623599
60623600
60623601
60623602
60623603
60623604
60623605
60623606
60623607
60623608
60623609
60623610
60623611
60623612
60623613
60623614
60623615
60623616
60623617
60623618
60623619
60623620
60623621
60623622
60623623
60623624
60623625
60623626
60623627
60623628
60623629
60623630
60623631
60623632
60623633
60623634
60623635
60623636
60623637
60623638
60623639
60623640
60623641
60623642
60623643
60623644
60623645
60623646
60623647
60623648
60623649
60623650
60623651
60623652
60623653
60623654
60623655
60623656
60623657
60623658
60623659
60623660
60623661
60623662
60623663
60623664
60623665
60623666
60623667
60623668
60623669
60623670
60623671
60623672
60623673
60623674
60623675
60623676
60623677
60623678
60623679
60623680
60623681
60623682
60623683
60623684
60623685
60623686
60623687
60623688
60623689
60623690
60623691
60623692
60623693
60623694
60623695
60623696
60623697
60623698
60623699
60623700
60623701
60623702
60623703
60623704
60623705
60623706
60623707
60623708
60623709
60623710
60623711
60623712
60623713
60623714
60623715
60623716
60623717
60623718
60623719
60623720
60623721
60623722
60623723
60623724
60623725
60623726
60623727
60623728
60623729
60623730
60623731
60623732
60623733
60623734
60623735
60623736
60623737
60623738
60623739
60623740
60623741
60623742
60623743
60623744
60623745
60623746
60623747
60623748
60623749
60623750
60623751
60623752
60623753
60623754
60623755
60623756
60623757
60623758
60623759
60623760
60623761
60623762
60623763
60623764
60623765
60623766
60623767
60623768
60623769
60623770
60623771
60623772
60623773
60623774
60623775
60623776
60623777
60623778
60623779
60623780
60623781
60623782
60623783
60623784
60623785
60623786
60623787
60623788
60623789
60623790
60623791
60623792
60623793
60623794
60623795
60623796
60623797
60623798
60623799
60623800
60623801
60623802
60623803
60623804
60623805
60623806
60623807
60623808
60623809
60623810
60623811
60623812
60623813
60623814
60623815
60623816
60623817
60623818
60623819
60623820
60623821
60623822
60623823
60623824
60623825
60623826
60623827
60623828
60623829
60623830
60623831
60623832
60623833
60623834
60623835
60623836
60623837
60623838
60623839
60623840
60623841
60623842
60623843
60623844
60623845
60623846
60623847
60623848
60623849
60623850
60623851
60623852
60623853
60623854
60623855
60623856
60623857
60623858
60623859
60623860
60623861
60623862
60623863
60623864
60623865
60623866
60623867
60623868
60623869
60623870
60623871
60623872
60623873
60623874
60623875
60623876
60623877
60623878
60623879
60623880
60623881
60623882
60623883
60623884
60623885
60623886
60623887
60623888
60623889
60623890
60623891
60623892
60623893
60623894
60623895
60623896
60623897
60623898
60623899
60623900
60623901
60623902
60623903
60623904
60623905
60623906
60623907
60623908
60623909
60623910
60623911
60623912
60623913
60623914
60623915
60623916
60623917
60623918
60623919
60623920
60623921
60623922
60623923
60623924
60623925
60623926
60623927
60623928
60623929
60623930
60623931
60623932
60623933
60623934
60623935
60623936
60623937
60623938
60623939
60623940
60623941
60623942
60623943
60623944
60623945
60623946
60623947
60623948
60623949
60623950
60623951
60623952
60623953
60623954
60623955
60623956
60623957
60623958
60623959
60623960
60623961
60623962
60623963
60623964
60623965
60623966
60623967
60623968
60623969
60623970
60623971
60623972
60623973
60623974
60623975
60623976
60623977
60623978
60623979
60623980
60623981
60623982
60623983
60623984
60623985
60623986
60623987
60623988
60623989
60623990
60623991
60623992
60623993
60623994
60623995
60623996
60623997
60623998
60623999
606239000
606239001
606239002
606239003
606239004
606239005
606239006
606239007
606239008
606239009
606239010
606239011
606239012
606239013
606239014
606239015
606239016
606239017
606239018
606239019
606239020
606239021
606239022
606239023
606239024
606239025
606239026
606239027
606239028
606239029
606239030
606239031
606239032
606239033
606239034
606239035
606239036
606239037
606239038
606239039
606239040
606239041
606239042
606239043
606239044
606239045
606239046
606239047
606239048
606239049
606239050
606239051
606239052
606239053
606239054
606239055
606239056
606239057
606239058
606239059
606239060
606239061
606239062
606239063
606239064
606239065
606239066
606239067
606239068
606239069
606239070
606239071
606239072
606239073
606239074
606239075
606239076
606239077
606239078
606239079
606239080
606239081
606239082
606239083
606239084
606239085
606239086
606239087
606239088
606239089
606239090
606239091
606239092
606239093
606239094
606239095
606239096
606239097
606239098
606239099
606239100
606239101
606239102
606239103
606239104
606239105
606239106
606239107
606239108
606239109
606239110
606239111
606239112
606239113
606239114
606239115
606239116
606239117
606239118
606239119
606239120
606239121
606239122
606239123
606239124
606239125
606239126
606239127
606239128
606239129
606239130
606239131
606239132
606239133
606239134
606239135
606239136
606239137
606239138
606239139
606239140
606239141
606239142
606239143
606239144
606239145
606239146
606239147
606239148
606239149
606239150
606239151
606239152
606239153
606239154
606239155
606239156
606239157
606239158
606239159
606239160
606239161
606239162
606239163
606239164
606239165
606239166
606239167
606239168
606239169
606239170
606239171
606239172
606239173
606239174
606239175
606239176
606239177
606239178
606239179
606239180
606239181
606239182
606239183
606239184
606239185
606239186
606239187
606239188
606239189
606239190
606239191
606239192
606239193
606239194
606239195
606239196
606239197
606239198
606239199
606239200
606239201
606239202
606239203
606239204
606239205
606239206
606239207
606239208
606239209
606239210
606239211
606239212
606239213
606239214
606239215
606239216
606239217
606239218
606239219
606239220
606239221
606239222
606239223
606239224
606239225
606239226
606239227
606239228
606239229
606239230
606239231
606239232
606239233
606239234
606239235
606239236
606239237
606239238
606239239
606239240
606239241
606239242
606239243
606239244
606239245
606239246
606239247
606239248
606239249
606239250
606239251
606239252
606239253
606239254
606239255
606239256
606239257
606239258
606239259
606239260
606239261
606239262
606239263
606239264
606239265
606239266
606239267
606239268
606239269
606239270
606239271
606239272
606239273
606239274
606239275
606239276
606239277
606239278
606239279
606239280
606239281
606239282
606239283
606239284
606239285
606239286
606239287
606239288
606239289
606239290
606239291
606239292
606239293
606239294
606239295
606239296
606239297
606239298
606239299
606239300
606239301
606239302
606239303
606239304
606239305
606239306
606239307
606239308
606239309
606239310
606239311
606239312
606239313
606239314
606239315
606239316
606239317
606239318
606239319
606239320
606239321
606239322
606239323
606239324
606239325
606239326
606239327
606239328
606239329
606239330
606239331
606239332
606239333
606239334
606239335
606239336
606239337
606239338
606239339
606239340
606239341
606239342
606239343
606239344
606239345
606239346
606239347
606239348
606239349
606239350
606239351
606239352
606239353
606239354
606239355
606239356
606239357
606239358
606239359
606239360
606239361
606239362
606239363
606239364
606239365
606239366
606239367
606239368
606239369
606239370
606239371
606239372
606239373
606239374
606239375
606239376
606239377
606239378
606239379
606239380
606239381
606239382
606239383
606239384
606239385
606239386
606239387
606239388
606239389
606239390
606239391
606239392
606239393
606239394
606239395
606239396
606239397
606239398
606239399
606239400
606239401
606239402
606239403
606239404
606239405
606239406
606239407
606239408
606239409
606239410
606239411
606239412
606239413
606239414
606239415
606239416
606239417
606239418
606239419
606239420
606239421
606239422
606239423
606239424
606239425
606239426
606239427
606239428
606239429
606239430
606239431
606239432
606239433
606239434
606239435
606239436
606239437
606239438
606239439
606239440
606239441
606239442
606239443
606239444
606239445
606239446
606239447
606239448
606239449
606239450
606239451
606239452
606239453
606239454
606239455
606239456
606239457
606239458
606239459
606239460
606239461
606239462
606239463
606239464
606239465
606239466
606239467
606239468
606239469
606239470
606239471
606239472
606239473
606239474
606239475
606239476
606239477
606239478
606239479
606239480
606239481
606239482
606239483
606239484
606239485
606239486
606239487
606239488
606239489
606239490
606239491
606239492
606239493
606239494
606239495
606239496
606239497
606239498
606239499
606239500
606239501
606239502
606239503
606239504
606239505
606239506
606239507
606239508
606239509
606239510
606239511
606239512
606239513
606239514
606239515
606239516
606239517
606239518
606239519
606239520
606239521
606239522
606239523
606239524
606239525
606239526
606239527
606239528
606239529
606239530
606239531
606239532
606239533
606239534
606239535
606239536
606239537
606239538
606239539
606239540
606239541
606239542
606239543
606239544
606239545
606239546
606239547
606239548
606239549
606239550
606239551
606239552
606239553
606239554
606239555
606239556
606239557
606239558
606239559
606239560
606239561
606239562
606239563
606239564
606239565
606239566
606239567
606239568
606239569
606239570
606239571
606239572
606239573
606239574
606239575
606239576
606239577
606239578
606239579
606239580
606239581
606239582
606239583
606239584
606239585
606239586
606239587
606239588
606239589
606239590
606239591
606239592
606239593
606239594
606239595
606239596
606239597
606239598
606239599
606239600
606239601
606239602
606239603
606239604
606239605
606239606
606239607
606239608
606239609
606239610
606239611
606239612
606239613
606239614
606239615
606239616
606239617
606239618
606239619
606239620
606239621
606239622
606239623
606239624
606239625
606239626
606239627
606239628
606239629
606239630
606239631
606239632
606239633
606239634
606239635
606239636
606239637
606239638
606239639
606239640
606239641
606239642
606239643
606239644
606239645
606239646
606239647
606239648
606239649
606239650
606239651
606239652
606239653
606239654
606239655
606239656
606239657
606239658
606239659
606239660
606239661
606239662
606239663
606239664
606239665
606239666
606239667
606239668
606239669
606239670
606239671
606239672
606239673
606239674
606239675
606239676
606239677
606239678
606239679
606239680
606239681
606239682
606239683
606239684
606239685
606239686
606239687
606239688
606239689
606239690
606239691
606239692
606239693
606239694
606239695
606239696
606239697
606239698
606239699
606239

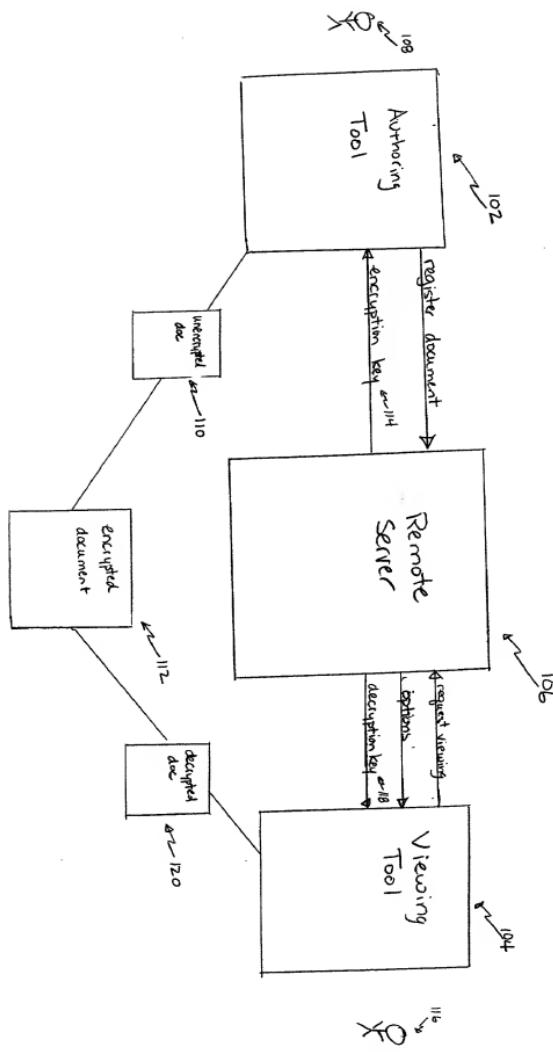
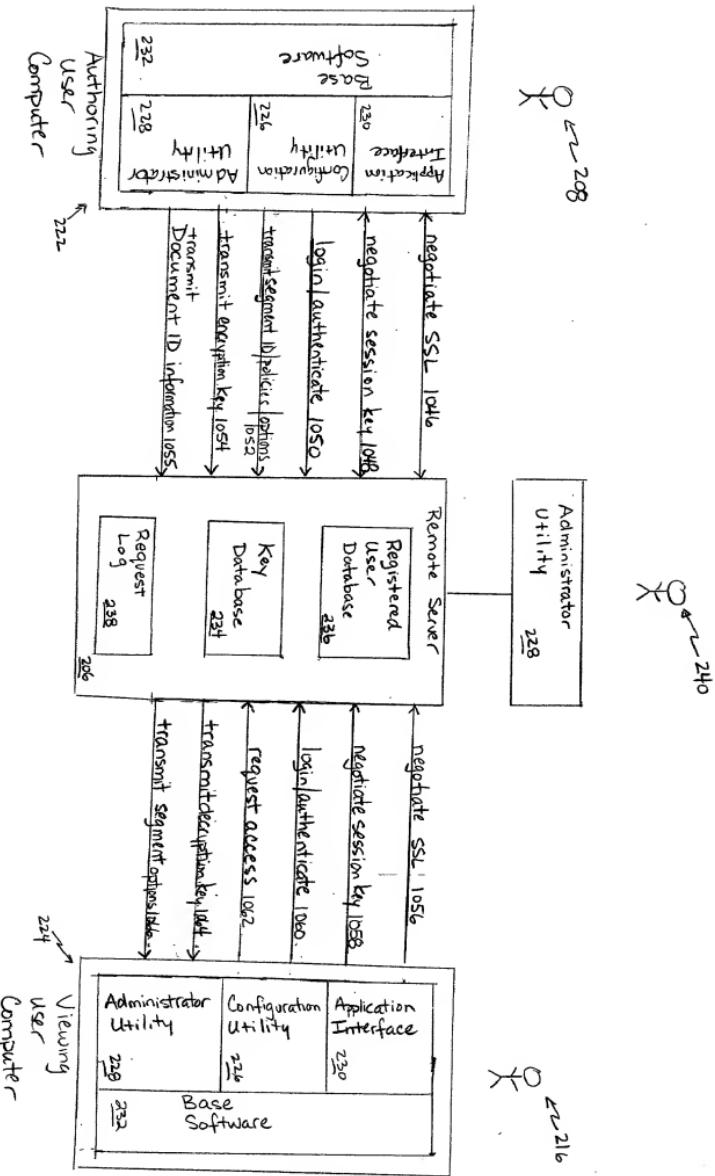


FIG. 1



F1G. 2

04321839-052899